ADMINISTERING USERS AND GROUPS (OSA-1)

MARCH 1998

VERSION (1.0)

TABLE OF CONTENTS

ADMINISTERING USERS AND GROUPS

OVERVIEW

This document outlines some of the basic AIX system administration functions for administering users and groups on an IBM RS6000 server housing the MUNIS financial system. Some functions, such as setting up MUNIS users, require the System Administrator to perform tasks in both AIX and MUNIS. This document deals only with system administration within the AIX operating system. For assistance with MUNIS system administration, see the document entitled ***MUNIS System Administration (MSA-1)*** in the ***MUNIS User Procedures Guide***.

MAINTAINING SECURITY

Security is of primary importance when administering a financial system. System security is only as good as the users' adherence to the security procedures the district has in place. Districts are encouraged to develop a systems security policy covering their entire data processing infrastructure. Each district's RS6000 has been configured by KDE with a base level of security to give a basic level of protection.

Access to the RS6000 is restricted by the use of passwords and related procedures. The **passwords** for AIX user accounts must:

1. Be a minimum of six (6) characters in length.
2. Expire every ninety (90) days.
3. Include three (3) characters different from the previous password.
4. Have no more than three (3) repeated characters.

The previous four passwords are retained for 26 weeks.

- To better protect the financial data, users should be instructed to assign passwords that cannot be easily guessed (e.g., their name, family member's name, place, hobby, etc.) and should not write their passwords on any visible objects (e.g., monitor, keyboard, etc.).
- It is very important that users have their own account on the RS6000. Individual user accounts provide an audit trail that identifies the author of changes to records within the system. Without individual user accounts, auditing a system can become extremely complex, if not impossible.
- When staff leave employment within a district, their user account(s) should be removed immediately from both the RS6000 and MUNIS. Other passwords which this person knows must be changed (e.g., root).

WARNING: ***Base security levels should be maintained at all times. Any modifications to security should comply with the district's security guidelines and complement base levels of security currently in place.***

OVERVIEW OF THE LOGIN (OR CONNECTION) PROCESS

Every user on the IBM RS6000 should have an individual login and telnet to MUNIS from their own personal terminal or PC. Under normal circumstances, staff should always login using their individual login id. Users should NOT login as “root” to access the MUNIS application.

The console of the IBM RS6000 is for performance of system management functions, and only the supervisor or "root" user should use the console. The console was never intended to be used as a terminal for accessing the MUNIS application.

The "root" or super user account is for system administration only. Staff who need “root” authority to temporarily perform some task (e.g., to transfer files such as the Monthly CERS file or the PSD file to diskette) should use the “su” command to switch user to root and not login as “root” directly.

Login steps are as follows:

1. In Windows 3.1, with the mouse, click on the **TNVT** icon in the **TCP Win Apps** group or **OnNet 2.0** group.

   In Windows 95, with the mouse, click on **Start** | **Programs** | **OnNet 2.0** | **TNVT** (or TNVT shortcut).

NOTE: ***The KDE standard communication software is FTP Software’s OnNet. This software provides telnet, ping, ftp, and server control (remote printing capabilities). Districts are responsible for obtaining OnNet license(s) for each PC using the software. See the document entitled OnNet Configuration (OSC-4) in the MUNIS User Procedures Guide for further information.***

2. Select **RS6000** from the Available Sessions list.

You will receive a login prompt from the IBM RS6000/AIX via the following process:

System Process	User Action	System Response
login		Displays login herald
	Enter User ID	Checks ID
		Displays password prompt
	Enter password	Checks password
		Displays message of the day
		Starts shell
		Provides shell prompt ($) to the user **or** places the user in the MUNIS application menu

SETTING UP AND CONFIGURING USERS

Establishing a new user with the appropriate permissions is a three-step process in AIX that is followed by several additional steps within MUNIS. See the document entitled ***MUNIS System Administration (MSA-1)*** in the ***MUNIS User Procedures Guide*** for instructions on establishing users in MUNIS.

In AIX, the System Administrator will perform the following steps to set up a user:

1. Add a user
2. Assign a password
3. Edit the user's profile (login script)

Once users have been set up in AIX, administration of existing users is seldom necessary. Occasionally you will need to:

- Modify user rights and login privileges
- Reset passwords
- Inactivate accounts
- Remove users

NOTE: ***Only the "root" user can perform user set-up functions.***

Adding a User

1. At the **$** prompt, type the following:

   smit mkuser (Press **Enter**.)

   The following screen is displayed:

```
 Session   Edit   Commands   Settings   Help
                                  Create User
Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                                    [Entry Fields]
* User NAME                                            []
  ADMINISTRATIVE User?                                  false
  User ID                                               []
  LOGIN User?                                           true
  PRIMARY Group                                         []
  Group set                                             []
  ADMINISTRATIVE Groups                                 []
  SU Groups                                             []
  HOME Directory                                        []
  Initial PROGRAM                                       []
  User information                                      []
  Another user CAN SU to user?                          true
  User CAN RLOGIN?                                      true
[MORE...13]

F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

2. Enter the user's **AIX login ID** in the **User NAME** field.

   NOTE: ***The AIX login ID can be a maximum of eight characters. Standard login names use the first letter of the user's FIRST NAME and the first seven letters of the LAST NAME. If this method results in a AIX login ID that is a duplicate of an existing ID, the user's middle initial is incorporated into the login name. The AIX login ID is later used as the User Code in MUNIS.***

3. Enter **Staff** as the **Primary Group**. (Press F4 to list choices.)

4. Enter **Staff, Informix** as the **Group Set**. (Press F4 to list choices.)

5. Press **Enter** to complete adding the user.

6. Press **Esc+0** to exit the utility.

The user's AIX login ID has now been established.

Assigning a Password

Assigning a password to a user account can be achieved by performing one of the following two (2) procedures:

A) Through **SMIT**:

1. At the **$** prompt, type the following:

   smit passwd (Press **Enter**.)

   The following screen is displayed:

```
 Session   Edit   Commands   Settings   Help

                          Change User Password

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
  User NAME                                            []



F1=Help             F2=Refresh          F3=Cancel           F4=List
Esc+5=Reset         Esc+6=Command       Esc+7=Edit          Esc+8=Image
Esc+9=Shell         Esc+0=Exit          Enter=Do
```

2. Enter the user's **AIX login ID** in the **User NAME** field and press **Enter**.

   The following screen is displayed:

```
Changing password for "username"
username's New password:
```

   The "**username**" refers to the AIX login ID of the user whose password is being changed.

3. Enter a **password** for the new user.

4. Enter the **password** for the user again for verification.

   NOTE: ***When the user enters the system for the first time, the system will ask for a new password. They should then enter a password of their choice.***

5. Press **F3** to return to the previous screen or **Esc+0** to exit the utility.

B) Through the **Command Prompt**:

1. Login as "root" on the IBM RS6000.
2. At the $ prompt type the following:

   passwd [**USERNAME**] (Press **Enter**.)

   ```
   Changing password for "username"
   username's New password:
   ```

   The "**username**" refers to the login ID of the user whose password is being changed.
3. Enter a new **password** for the user.
4. Enter the new **password** again for verification.

Editing the User's dot Profile

When the AIX system creates a new user, it also creates a **directory** for that user and a default **.profile** (referred to as a dot profile or login script). The dot profile is executed by the shell automatically at login and contains commands you want executed each time the user logs in. This file is located in each user's home directory.

A dot profile can be copied from another user or the default dot profile can be edited. The following example demonstrates how to add the **Menu** and **Exit** commands to the dot profile. The Menu command added to the dot profile will take the user directly to the MUNIS menu screen after logging in. Exit will terminate the Telnet session when the user exits from MUNIS.

1. At the $ prompt type:

   cd /home/username (Press **Enter**.)

   Username refers to the AIX login ID of the user whose dot profile is being edited. This command will change to the user's "home" directory where the dot profile is located.
2. At the $ prompt, type:

   vi .profile (Press **Enter**.)

   This command will activate the vi editor and open the user's dot profile. See ***Appendix A Basic VI Editor Commands***.
3. Using the arrow keys, move the cursor to the last character on the last line. This is the insertion point.
4. Press **ESC** and **o** (lowercase) to insert a new line.
5. Type **menu** and press **Enter**.
6. Type **exit** and press **Enter**.
7. Press **ESC** and type **:wq**

This will save the changes made to the .profile and close the file.

8. Type **cd**.

If the user's TNVT screen setting "**Exit on Disconnect**" is turned on, the TNVT window will also close on exiting MUNIS.

Inactivating a User Account

When a user is due to leave the office for an extended time (e.g., vacation), it is a good idea to inactivate that user's account. Deactivation of the user's account acts as a security measure that allows no other users to use that account while they are out of the office. This type of procedure is also appropriate for creation and use of temporary user accounts.

1. At the $ prompt, type:

   smit user (Press **Enter**.)

2. Select **Lock/Unlock a User's Account**.

3. Enter the **user's id.**

4. Press the **tab** key until "**Is this users Account Locked?**" says "**True**".

5. Press **Enter.**

Removing a User Account

User accounts should be removed when employees have left employment. (You should also remove their MUNIS login as well.)

1. At the $ prompt, type:

   smit user (Press **Enter**.)

2. Select **Remove user**.

3. Enter the **user's id**.

4. Press **Enter**.

After removing the user's account with SMIT, their home directory and contents should be removed.

1. Login as "root".
2. Issue the command " **cd /home** ".
3. Issue the command " **rm -r** [**USERNAME**] ".
4. Logout.

SETTING UP AND CONFIGURING USERS IN GROUPS

Groups are an excellent way to manage your system and printing. Two important groups that are part of the standard configuration are "Staff" and "Informix." "**Staff**" is a primary group to which all users on the RS6000 belong because it enables the sharing of files. The "**Informix**" group is also critical because it gives users the right to access the Informix data base that houses MUNIS data. AIX has a default group called "**printq**". Anyone belonging to this group can stop and start queues and cancel print jobs of other users on the system. A user who is not a member of this group can only cancel, delete, or print their own print jobs.

To Set Up Users in Groups:

1. At the **$** prompt type the following:

   smit group (Press **Enter**.)

The following screen is displayed:

```
 Session   Edit   Commands   Settings   Help

                              Groups
Move cursor to desired item and press Enter.

  List All Groups
  Add a Group
  Change / Show Characteristics of a Group
  Remove a Group

F1=Help          F2=Refresh         F3=Cancel        Esc+8=Image
Esc+9=Shell      Esc+0=Exit         Enter=Do
```

2. Select **Change / Show Characteristics of a Group**.

The following screen is displayed:

```
Session   Edit   Commands   Settings   Help

                      Change Group Attributes

Type or select a value for the entry field.
Press Enter AFTER making all desired changes.

                                                  [Entry Fields]
  Group NAME                                  []                  +



F1=Help           F2=Refresh         F3=Cancel          F4=List
Esc+5=Reset       Esc+6=Command      Esc+7=Edit         Esc+8=Image
Esc+9=Shell       Esc+0=Exit         Enter=Do
```

3. Enter a **Group NAME** (e.g., printq) or press **F4** and select a group.

4. Enter a **USER list** or press **F4** to select the users that you want to add to this group.

5. Press **Enter** to complete adding users to the group.

6. Press **Esc+0** to exit the utility.

PERMISSIONS (File / Directory)

File permissions are used to protect files from unauthorized access.

Permissions Diagram

```
-rwxrwxr-x 1  root      system   819      Feb 12   21:08    .profile
rwx           rwx           r-x                             r  =  read     =  4
-------       -------       -------                         w  =  write    =  2
   |             |             |                            x  =  execute  =  1
   |             |             others
   |             group
   user
```

For an ordinary file

r	can look at contents of the file	(cat, pg, more)
w	can change or delete contents of the file	(vi)
x	can use the filename as a command	(ksh)

For a directory

r	can list files in the directory	(ls, li)
w	can create/remove files in the directory	(x required!)
x	can be “in” the directory	(cd to it or access its files or sub-directories)

Permissions Command

$ **chmod** [**MODE**] [**FILENAME**]

This command is used to grant users read, write, and/or execute permissions on files and/or directories.

Example:

1. At the $ prompt type:

   chmod 750 /home/[**USERNAME**]**/.profile** (Press **Enter**.)

2. At the $ prompt type:

   cd /home/[**username**] (Press **Enter**.)

3. At the $ prompt type:

   ls -l .profile (Press **Enter**.)

The permissions on the file **.profile** now reflect: rwx r_x ___ or 7 5 0

APPENDIX A

Basic VI Editor Commands

As a system administrator, there are times when you have no choice but to use the vi editor. Actually, vi is very efficient to use once you become familiar with it. To exploit that efficiency, this list of basic commands is provided. The following are the minimum basic commands that will help you get IN, get AROUND and get OUT of vi.

Entering Text

When you first get into vi, you are in the COMMAND mode. In order to type your text, you must give a COMMAND to enter TEXT mode. Those commands are either **a**, **i**, or **o**.

- **a** appends text after the cursor
- **i** inserts text before the cursor
- **o** opens a new line and puts text in it

Moving Around

To move AROUND on the screen, try using your arrow keys. If they don't move the cursor around, place the fingers of your right hand over the **h**, **j**, **k** and **l** keys. These keys will move you left, down, up and right, **if** you are in COMMAND mode. (See below.)

- **h** left
- **j** down
- **k** up
- **l** right

Back to Command Mode, Saving and Exiting

To move around in your file, execute any command, or to save your work, go back to COMMAND mode by pressing **ESC**.

- **SAVE** your changes with **:w** — **w** writes the vi buffer to the file.
- **EXIT** vi with **:q** — You can also type **:wq** to write and quit in one step.
- **PANIC** (just get out) with **:q!** — **q!** will leave vi without changing anything.

Undo and End of Word

Two more useful commands are **u** and **e**.

- **u** is the **UNDO** command. It will undo your last action.
- **e** moves you directly to the **END** of the next word.

Miscellaneous Commands

- **x** deletes a character.
- **r** replaces a character.
- / lets you enter a search string. (Press **Enter** to find it.)
- **n** finds the next occurrence of the string you just searched for.